Claims

What is claimed is:

1. A method of authenticating a self-authenticating document, comprising the steps of:

processing machine-readable data on said self-authenticating document to obtain digital signature data and a public key certificate;

processing said public key certificate to obtain public key certificate data including an authentic public key;

assembling critical document data from said self-authenticating document, wherein said critical document data includes at least magnetic ink character recognition (MICR) data printed on said self-authenticating document;

determining whether an authentic personal identification number (PIN) is available for appending to said critical document data;

wherein, if said authentic PIN is available;

appending said authentic PIN to said critical document data to create an authenticatable data string; and,

applying said authentic public key to said digital signature data to validate said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

2. The authenticating method of claim 1, wherein said self-authenticating document is a personal check, and wherein said critical document data includes ASCII text printed on said personal check.

3. The authenticating method of claim 1, further comprising the steps of:

determining whether a first digital signature is present in said digital signature data, if it is determined that said authentic personal identification number (PIN) is not available;

applying said authentic public key to said digital signature data to validate said critical document data, wherein said self-authenticating document is authenticated if said critical document data is validated.

4. The authenticating method of claim 3, wherein if it is determined that said authentic PIN is not available and that said first digital signature is not present in said digital signature data, further comprising the steps of:

determining whether a second digital signature is present in said digital signature data, and,

if said second digital signature is present;

generating a plurality of PINs;

appending each of said plurality of PINs to said critical document data to create a plurality of verifiable data strings; and,

applying said authentic public key to said second digital signature in order to validate one of said verifiable data strings as said authenticatable data string and to authenticate said self-authenticating document.

5. The authenticating method of claim 4, wherein said step of generating PINs is carried out in a document reading system executing a PIN-generating algorithm.

6. The authenticating method of claim 3, wherein said machine-readable data is bar-code data, said machine-readable data processing step including the substeps of:

retrieving said bar code data from said self-authenticating document; and,

parsing data fields in said bar code data to obtain at least said public key certificate, said digital signature data, and k, where k, is the total number of bytes in said bar code data.

7. The authenticating method of claim 3, wherein said public key certificate data processing step includes the substeps of:

validating said public key certificate with a third-party public key; and,

parsing said public key certificate to obtain said authentic public key;

8. The authenticating method of claim 7, wherein said public key certificate includes a third-party digital signature, and wherein said public key certificate validating step further comprises the substep of applying said third-party public key to said third-party digital signature.

9. The authenticating method of claim 7, wherein said third party is a certificate authority.

10. The authenticating method of claim 7, wherein said public key certificate is comprised of m bytes, and wherein said public key certificate parsing substep includes the further substeps of:

retrieving at least a first byte, c_1 , of said m bytes from said public key certificate, wherein said at least a first byte c_1 is a binary representation of said number of bytes m in said public key certificate;

determining whether said binary representation of said number of bytes m in said at least a first byte c_1, is greater than the number of bytes of data in said digital signature data, n;

retrieving the remainder of said m bytes, if said determining step determines that said at least a first byte c_1 is greater than the number of bytes of data in said digital signature data, n; and,

applying said authentic public key to said digital signature data in order to verify said at least one of said first and second digital signatures.

11. The authenticating method of claim 10, wherein said public key certificate parsing substep includes the further substeps of:

retrieving public key validity date data from said public key certificate;

determining if said public key validity date data is within an accepted date range; and,

validating said public key certificate with said public key validity date data, if said public key validity date data is within said accepted date range.

12. The authenticating method of claim 11, wherein said public key certificate parsing substep includes the further substep of:

issuing an alert if said public key validity date data is not within an accepted date range.

13. The authenticating method of claim 12, wherein said public key certificate parsing substep includes the further substeps of:

deciding whether to validate said public key certificate if said public key validity date data is not within an accepted date range, by checking guidelines issued by said third party.

14. The authenticating method of claim 12, wherein said public key certificate parsing substep includes the further substeps of:

deciding whether to validate said public key certificate if said public key validity date data is not within an accepted date range, by consulting a public key certificate database.

15. The authenticating method of claim 3, further comprising the step of :

presenting said self-authenticating document by an owner of said self-authenticating document to a commercial entity for authentication, wherein said presenting step is carried out prior to said machine-readable data processing step.

16. The authenticating method of claim 15, wherein said authentic PIN-determining step further includes the substep of:

determining whether an owner of said self-authenticating document is available to input said authentic PIN, wherein said PIN-availability step determines that said authentic PIN is not available if said owner of said self-authenticating document is not available.